

REMARKS

In the outstanding Office Action, the Examiner rejected claims 1-4 and 6-9 under the judicially created doctrine of obviousness-type double patenting as being an obvious variation of claims 1-22 of U.S. Patent No. 6,834,333 to Yoshino et al. ("Yoshino"); and rejected claims 1-4 and 6-9 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,673,319 to Bellare et al. ("Bellare")¹. No claims are amended herein, and claims 1-4 and 6-9 remain pending.

I. Obviousness-Type Double Patenting

Applicants respectfully traverse the rejection of claims 1-4 and 6-9 under the judicially created doctrine of obviousness-type double patenting on the grounds that the Examiner has failed to establish that claims 1-4 and 6-9 of the present application define an obvious variation of the invention defined in claims 1-22 of Yoshino.

As stated in MPEP § 804 (internal citations omitted):

[a] double patenting rejection of the obviousness-type is "analogous to [a failure to meet] the nonobviousness requirement of 35 U.S.C. § 103" ... [t]herefore any analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. § 103 obviousness determination ... [a]ny obviousness-type double patenting rejection should make clear:

(A) The differences between the inventions defined by the conflicting claims - a claim in the patent compared to a claim in the application; and

(B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim in

¹ The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement of characterization in the Office Action.

issue is an obvious variation of the invention defined in a claim in the patent.

In rejecting claims 1-4 and 6-9, the Examiner asserts:

all elements of claims 1-4 and 6-9 correspond to the claims 1-22 of the patent claims, except in the instant claims 1, 6, 7, 8 and 9, cryptosystem means received, as cryptosystem keys for performing cryptosystem processing ... is referred in the patent claims 1, 4, 6, 11, 12, as an integrity check value [and] it would have been obvious to one having ordinary skill in the art to recognize that providing the cryptosystem keys ... is equivalent to generating an integrity check value. Office Action, page 3-4 (emphasis added).

Applicants respectfully disagree with the Examiner's assertions. Claim 1, for example, recites a data storage device including "executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode using a storage key stored in said data storage device." Claims 1-22 of Yoshino fail to recite at least "first and second set of keys," "cipher block chaining (CBC) mode," and "a storage key," as recited in claim 1.

The Examiner appears to assert that features such as these are equivalent to the claimed "generating an integrity check value," as recited in Yoshino. The Examiner, however, has failed to provide any reasons why providing cryptosystem keys, or using CBC encryption, is an obvious variation of "generating an integrity check value," as required by MPEP § 804.

Accordingly, the Examiner has failed to establish that Applicants' claims 1-4 and 6-9 define an obvious variation over claims 1-22 of Yoshino. Applicants therefore

respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under the judicially created doctrine of obviousness-type double patenting.

II. Rejection Under 35 U.S.C. § 102(b)

Applicants respectfully traverse the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b) because Bellare, as relied on by the Examiner, does not anticipate claims 1-4 and 6-9.

Claim 1, for example, recites a data storage device including an encryption means for creating encrypted keys by “executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode using a storage key stored in said data storage device.” Bellare fails to teach at least the claimed encryption means.

Bellare discloses a method of encryption wherein:

encryption involves using the plaintext string and a first key to compute a message authentication code. The routine continues by using the message, a second key, *and the message authentication code* to produce an enciphered string that depends substantively *on the message authentication code*. Bellare, col. 6, lines 55-60 (emphasis added).

Even if Bellare’s first and second keys could be reasonably construed as corresponding to Applicants’ claimed “first and second set of keys,” Bellare discloses encrypting a plaintext string with the first string, and then encrypting a second string with the result of the encrypted first key and plaintext message, and the message. Bellare, however, does not disclose “executing encryption ... using a storage key stored in said data storage device,” as recited in claim 1 (emphasis added).

Because Bellare fails to teach each and every element recited in independent claim 1, Bellare does not anticipate independent claim 1. Accordingly, Applicants respectfully submit that independent claim 1 is allowable over Bellare, and claims 2-4 are allowable at least due to their dependence on claim 1.

Claims 6-9, while of different scope, recite elements similar to those recited in independent claim 1. For example, claim 6 recites a data recording method including “encryption processing is executed on said first and second set of keys in the CBC mode using a storage key stored in said data storage device.” Claim 7 recites a data playback method including “executing encryption processing in the CBC mode using a storage key unique to said data storage device on an integrity-check-value generating key of data to be stored in at least one of the sectors” (emphasis added). Claim 8 recites a program providing medium including a computer program for “executing ... encryption processing in the CBC mode on ... a second set of keys correlated with integrity-check-value generating keys of data to be stored in at least one of the sectors, the encryption processing executed using a storage key stored in said data storage device” (emphasis added). Claim 9 recites a program providing medium including a computer program for “executing encryption processing in the CBC mode using a storage key unique to said data storage device on an integrity-check-value generating key of data to be stored in at least one of the sectors” (emphasis added). For at least the reasons given above with respect to claim 1, most notably that Bellare fails to execute encryption “using a storage key unique to said data storage device,” Applicants submit that claims 6-9 are also allowable over Bellare. Accordingly,


Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b).

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 18, 2006

By: 
Darrell D. Kinder, Jr.
Reg. No. 57,460